By e-mail/Speed-Post

Govt. of India
Ministry of Finance
O/o Pr. Chief Controller of Accounts
Central Board of Indirect Taxes and Customs
Expenditure Coordination Section `
A.G.C.R. Building, I. P. Estate
New Delhi-110002

Pr.CCA/CBIC/Coord-Expdr/Circular-Instruction/Vol.I/2022-23/258 Dated:- 24/02/2023

CIRCULAR

Sub : IT Security advisory for State Governments and agency users.

Please find enclosed herewith PFMS(HQ) O.M No. V-14014/5/2021-PFMS/C.No-8766/7103 dated 20.02.2023 on the above cited subject.

All Zonal Heads of CBIC are requested to direct respective PAOs under their administrative control for strict compliance of the IT Security instructions contained in aforesaid O.M.

This issues with the approval of the Competent Authority.

Encl : As above

Yours faithfully,

(Lakshman Dubruwal)
Sr. Accounts Officer

To:

1. Dy.CA, North Zone, CBIC, New Delhi
2. Dy.CA, O/o CA(WZ), CBIC, Mumbai
3. ACA, O/o DCA(EZ),CBIC, Kolkata
4. Dy. CA, O/o DCA(SZ), CBIC,Chennai
5. All PAO of North Zone

Copy to :

1. Sr. PS to Pr. CCA,CBIC
2. PS to CCA, CBIC
3. PA to DCA, CBIC
4. Sr. AO(Admn), CBIC
5. Sr. AO(ITD)-requested to upload on the ARPIT portal.

V-14014/5/2021-PFMS/C.No-8766/ 7103
GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF EXPENDITURE
CONTROLLER GENERAL OF ACCOUNTS
PUBLIC FINANCIAL MANAGEMENT SYSTEM (HQ)

3rdFloor, Shivaji Stadium Annexe
New Delhi-110001
Dated: - 20 .02.2023

Office Memorandum

Sub: IT security advisory for State Governments and agency users.

A reference is invited to this Office OM No.V-14014/5/2021-PFMS/C.No-8766/1898 dated 14.07.2022 vide which an IT security advisory for State Governments and agency users of PFMS was issued. Now, PFMS in consultation with Department of Expenditure (PFS Division), M/o Finance has prepared an IT security related instructions for State as well as agency users while using SNA accounts.

All the PFMS users are advised to ensure strict compliance of the advisory at all the respective levels and put in place a regular monitoring mechanism for the same.

This issues with the approval of the Competent Authority.

Rahul Garg
20/02
(Rahul Garg)
ACGA, PFMS (Tech.)

To:

1. All State Government Departments / Agencies.

Copy to:

1. PS to all Chief Secretaries/Principal Finance Secretaries of State Governments.
2. PS to FAs/Pr.CCAs/CCAs/CAs(I/C) of all Central Ministries/Departments.
3. PS to Addl. CGA, PFMS Division
4. PS to Addl. Secretary, PFS, D/o Expenditure, M/o Finance.
5. PS to Jt.CGA (JKP/CVP), PFMS Division.
6. PS to Director, D/o Expenditure, M/o Finance.
7. DDG, NIC, PFMS Division
8. Director Treasury/SSM's of all state Departments, All State Govt. Departments
9. All State Directorates for wide circulation.
10. Sr.AO (Roll-out / CGA) for uploading on PFMS / CGA website.

ANNEXURE-1

IT security related instructions while using SNA Accounts

These guidelines are prepared to disseminate Information Security best practices, to avoid the risks of cyber-attacks and any fraudulent activity.All users of state government, agency, sub-agency, and vendor are hereby advised to ensure the adoption of the following safeguards while accessing PFMS portal through their systems (Desktop/Laptops).

1 User Creation and Management

i. New user registration is to be initiated by the concerned approving authority in PFMS.

ii. For new user registration of State officials dealing with the SNA module of PFMS, only the NIC/GOV /State Govt email id should be used. Users already registered on PFMS with a Non-NIC/GOV email ID should be shifted to NIC/GOV / State Govt email ID. Non-compliant users' accounts should be deactivated immediately.

iii. The list of SNA users in PFMS i.e. 'SFD/SPCU/SSM/DA/DO/Agency admin/agency approver level2' may be reviewed and updated on aregular basis by authorized approvers. If any user is found to be no longer in position then the same may be deactivated immediately, to keep the active users list up to date.

iv. Implement a high level of verification i.e. by scrutiny/ credential check at the time of registration of vendor/support users' i.e. recruit from the outsourced agency.

v. SNA configures bank name and account mapping shall be carried outby SSM should be through designated system only.

vi. While creation of the child agency - Parent Agency should verify the mobile number /Email ID and other information provided by the sub- agency.

vii. Creation of multiple Parallel agency admin IDs should be discouraged.In case of Agency Admin authorizes parallel agency admin ID creation,it should be allowed for a short duration and immediately discontinued after the use.

2 Password Management

i. All systems-level passwords must be changed at least every 60 days.

ii. All users create a strong password with a minimum length of 8 and should contain alphabets (one upper & one lower case), numbers, and special characters.

iii. Password should not be similar to a user name or part of the user name.

iv. Password should not be similar to personal email ID passwords.

v. New Passwords should not be identical to the last three old passwords.

vi. To ensure that only the user knows the password, he/she should change the password at the time of the first Login into the system.

vii. Passwords should not be stored in readable form in computers, notebooks, notice boards, or in any other location where unauthorized persons might discover or use them.

viii. Always decline the use of the "Remember Password" feature whereverit is prompted by the applications.

ix. Do not share passwords while exchanging information over email/ mobile with PFMS(HQ)/ Helpdesk team.

x. Registered users should not share their email IDs\passwords with colleagues / anyone, any legal issue arising out of sharing the password/ User Ids shall be the liability of the owner.

xi. In case of any suspicion of the password being compromised, it mustbe changed immediately by logging into the PFMS portal. The user can also check their login history (Past IPs) used to access PFMS via the "login History" hyperlink in the top right under their PFMS user name.

xii. Do not share system passwords or Wi-Fi passwords with any unauthorized persons.

xiii. All users should ensure that the desktop must be locked (the shortcut 'Window+L') at the time of leaving their room/workstation.

3 DSC and Payment Processing

i) SNA Agency Admin while approving DSC should:

- Check the validity of DSC.
- Certified DSC is being used by the agency.
- Proper configuration of signatory levels as per the amount ranges.
- Procured from Controller of Certifying Authority approved empaneled vendors.

ii. The authorized DSC key owner should not share his/her digital signature key. If any legal issue arising because of the share of the DSC key shall be the liability of the owner. Any loss/theft of the DSC key should be reported and disabled immediately.

iii. The default PIN/password of the DSC Key must be changed and practice may be adopted for regular changing of its PIN/Password.

iv. User must thoroughly check each payment file of a batch with the corresponding physical bills before putting the Digital signature.

v. Users are not allowed to use digital signatures for making payments from the computers installed outside their office locations. Agency shall issue an instruction to their users

vi. DSC activation\deactivation must be controlled by agency admin, in case of DSC is not being used for particular schemes then it should be deactivated by agency admin for those schemes to prevent misuse.

vii. Daily monitoring of Payment success/failures initiated by DO/DA's ofthe SNA module.

viii. All guidelines stipulated to be followed for making payments should be strictly adhered to and verification against physical documents shouldbe done at all levels unless stipulated by explicit directions for use of electronic mediums.

4 Bank Reconciliation and Internal Check / Audit:

i. Agency Admin should weekly review the following: -

- Failure payment and find out the failure reasons.
- Verify all the successful payments transferred whether to correct beneficiary.
- Bank account balances should be matched against the actual passbook balances.

ii. Parent Agency (Funding agency) must conduct surprise audits on the financial activities of its child agencies once in a month.

iii. Agency Admin regularly audit the holding account fund transfers and settlement in time to avoid penalties. In case, no settlement is being done within the stipulated time, the amount shall be credited back to the SNA account.

iv. Funding/Parent Agency to ensure "Saving bank account" should be used during the scheme registration and a non interest bearing account should be used for holding account.

5 Record Management

i. The log of the approved agencies/vendors/ individuals list along with bank account details and other credentials in soft and physical formshall be maintained by Parent Agency/SSM/ Agency Admn. The same may be reviewed / updated on regular basis.

ii. Parent agency / Agency Admn should maintain the users details / DSC enrolled details repository, which should be monthly reviewed to incorporate all user Ids activation/deactivation.

6 System and External Storage

i. Usage of External Storage media and communication devices may be avoided as far as possible. Instead designated system can be put in place for connecting with external devices after antivirus & malware scans. The unregulated use of devices (like Pen drives, mobile phone, etc.) may cause transmission of malicious files from devices and compromise the computers/network making them vulnerable to cyber attacks..

ii. User should save critical data and files on the secondary drive (ex: - d:\). And take regular backups.

iii. When users leave the office, ensure that user should turn off their computers and printers.

iv. Do not use any authorized remote administration tools (ex: - Team viewer, Ammy admin, Anydesk, etc).

v. Users shall ensure that the unnecessary Apps related to cloud storage (DropBox, Google Drive, etc.) are not installed in the system.

vi. Use Licensed and authorized software only.

vii. The session of PFMS may be logged out if not in use. An idle session may lead to unauthorized access and load on the server.

7 Exit Policy Standard

i. At the time of relieving of any state/agency/vendor/support user (upon transfer/superannuation) his/her digital signature and system credentials should be deactivated.

ii. Ensure the user must return the assigned DSC to his/her immediate reporting officer at the time of leaving.

iii. Ensure the user must share his system details with the immediate reporting officer at the time of leaving.

iv. While relieving DA/DO user, his contact details must be changed or deleted by the agency admin, so that user cannot misuse the credentials for associated schemes.